UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/459,493	12/13/1999	MOSHE RUBIN	P-9038-US	1209

7590 05/30/2006

Eitan Law Group
c/o Landon IP, Inc.
Suite 450
1700 Diagonal Road
Alexandria, VA 22314

EXAMINER	
COLIN, CARL G	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 05/30/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/459,493	RUBIN ET AL.	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 May 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-14,16-27,29-36,38-53,55-66 and 68-80* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-14,16-27,29-36,38-53,55-66 and 68-80* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *13 December 1999* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. In response to communications filed on 3/2/2006, the following claims 1, 3 - 14, 16 - 27, 29 - 36, 38 - 53, 55 - 66 and 68 - 80 are presented for examination.

2. Applicant's arguments, filed on 3/2/2006, with respect to the rejection of claims 1, 14, 27, 36, 45, 50, 53, and 66, have been fully considered, but they are not persuasive. In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, Mast is concerned with method for protecting image display. Mast mentions that some prior art utilizing masking of portions of visual output but fails to design for security purposes (column 2, lines 13-25). Dwin reference discloses a technique for protecting displayed information by modifying the least significant bit to generate control data (see column 8, lines 45-62). There is suggestion that an alternative to storing the entire frame buffer image (display image) would be to store data representing only the information to be protected in the lock buffer (non-display memory) (column 7, lines 45-48) and discloses "once the lock data is placed in the lock buffer, subsequently writing into the frame buffer (video memory) is controlled by the contents of the

lock buffer; protection data is read in the lock buffer and control signal is generated to write data in the frame buffer section, because data to be protected is identified and already protected, it is obvious that setting of the bits can be applied before writing into the frame buffer. "The specific structure of information shown in the frame buffer is only an example and it is well known within the skill of the art to provide different arrangements of the data" (column 7, lines 25-37). It is also a design choice to modify the bits in any memory area of the device such as ROM, cache memory, or any other well-known in the art, rather than modifying the bits in the frame buffer memory (video memory) because the source of the image may require that the image is protected at all times as in copyright protection, client/server, etc. Also, Mast is concerned in having the image present in the video memory unprotected as it is susceptible to piracy. One within the skill of the art would be motivated to utilize the method of Dwin modifying the bits before the image is present in the video memory so it is not susceptible to piracy when it is displayed as suggested by Mast. In addition, it is in the knowledge generally available to one of ordinary skill in the art that besides encoding the bit as a protection scheme, changing the least significant bit of pixels data sometimes called (data hiding in images) provides protection of the image while the degradation of the quality of the image can be prevented and this technique may be performed in any memory device which means prior to being received in the video RAM, as taught in the cited references and in applicant's disclosure by Rhoads. Applicant is provided with additional prior art for support of modifying least significant bit technique prior to being in a video RAM. As explained above, modifying least significant bits of a pixel data prior to being received in the video RAM is obvious in view of the prior art. Upon further consideration,

claims 1, 3-14, 16-27, 29-36, 38-53, 55–66, and 68-80 remain rejected under 35 U.S.C. 103(a) as being unpatentable over Mast in view of Dwin.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3.1 **Claims 1, 3-14, 16-27, 29 - 36, 38-53, 55–66, and 68-80** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 5,881,287 to **Mast** in view of US Patent 5,986,676 to **Dwin et al**.

3.2 **As per claim 1**, **Mast** substantially teaches a method for protecting digital images from being copied from a video RAM, (see column 3, lines 25-34 and column 9, lines 60-67). **Mast** discloses the step of transmitting stored pixel data from a computer memory to a video RAM (column 3, lines 25-57). As defined in the dictionary, the pixels are the basic units of the composition of the image disclosed by **Mast**. **Mast** also discloses the step of identifying

protected image within the image in memory that meets the recitation of identifying the protected pixel data within the stored pixel data (see column 3, lines 30-49; and lines 49-57; and column 10, lines 57-61). **Mast** discloses in prior art (columns 1-3) many examples of modifying pixel data prior to arrival at the video RAM. **Mast** further discloses the steps of modifying pixel data by encryption before transmitting to end users, prior to its being received by the video RAM, thereby generating modified pixel data within which individual pixel datum is recognizable as being protected or unprotected (see column 7, lines 34-47); and after instruction to copy pixel data from the video RAM, replacing individual pixel datum that is recognized as being protected, with substitute pixel datum (column 3, lines 30-49, column 9, lines 59 et seq., and column 10, line 53 through column 11, line 1). **Mast** discloses that encryption fails to protect pixel data within the video memory because of the need to be displayed (see column 1, lines 62-66). **Mast** discloses that prior art technique may be applied to provide protection of data until displayed and the present invention will continue to provide security for data transfer request being in the video memory and teaches means of preventing copying of images stored in the picture store of the video display (see abstract and column 3, lines 25-58). **Mast** combines encryption technique as an example of prior art protection prior to placing the image in the video memory with his inventive features of providing image display protection including preventing copying of image from the screen to protect the image from theft. **Mast** mentions that other prior art utilizes masking of portions of visual output but fails to design for security purposes (column 2, lines 13-25). **Mast** does not explicitly disclose prior art technique using least significant bits technique for providing protection of pixels data. However, **Dwin et al** in an analogous art discloses a technique for protecting displayed information by modifying the least significant bit to generate

control data (see column 8, lines 45-62) and further teaches reading protection data in the lock buffer (non-display section) to determine location in the frame buffer (video memory) where information can be written and ultimately on the display screen (column 3, lines 30-46), which meets the recitation of modifying least significant bits of stored pixel data prior to it's being received by the video RAM, (see also column 7, lines 45-61 and column 8, lines 15-35 and lines 45-63; column 5, lines 22-28). There is suggestion that an alternative to storing the entire frame buffer image (display image) would be to store data representing only the information to be protected in the lock buffer (non-display memory) (column 7, lines 45-48) and discloses "once the lock data is placed in the lock buffer, subsequently writing into the frame buffer (video memory) is controlled by the contents of the lock buffer; protection data is read in the lock buffer and control signal is generated to write data in the frame buffer section, because data to be protected is identified and is already protected, it is obvious that setting of the bits can be applied before writing into the frame buffer. "The specific structure of information shown in the frame buffer is only an example and it is well known within the skill of the art to provide different arrangements of the data" (column 7, lines 25-37). **Dwin et al** further discloses recognizing individual pixel datum as being protected or unprotected based on the least significant bits of the datum without comparison to a template of pixel locations, for example (see column 7, lines 45-61 and column 8, lines 15-35 column 5, lines 22-28) with the advantage that it enables to know which location of the data to be displayed must be protected by setting all the protect bits corresponding to the pixels in the destination for the object (see column 8, lines 14-35 and lines 45-67). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Mast** by modifying least significant bits of stored

pixel data prior to its being received by the video RAM and recognizing individual pixel datum as being protected or unprotected based on the least significant bits of the datum as taught by **Dwin et al.** (see column 7, lines 10-40). One skilled in the art would have been motivated to do so because Mast suggests having the image present in the video memory unprotected is susceptible to piracy and one of ordinary skill of the art would have been motivated to utilize the method of **Dwin et al** of modifying the bits before the image is present in the video memory so it is not susceptible to piracy when it is displayed as suggested by **Mast**. Contrarily to some prior art that provides protection only before displaying data as mentioned in Mast, **Dwin et al** also provides the advantage where data to be displayed and data currently displayed can remain protected by modifying significant pixels to provide control and identification of data locations that need to be protected before displaying on the screen, wherein any portion of the screen may be so protected using a lock protect bit that corresponds to any pixel data that needs to be protected (see column 7, lines 38-61 and column 8, lines 14-35, 45-67), selected areas of the screen can be protected against overwriting (column 7, lines 34-38).

As per claims 3, 29, and 55, Dwin et al. discloses wherein pixel data includes red, green, and blue color components said modifying sets the least significant bits within any pixel data of any color that meets the recitation of limitation of wherein pixel data includes red, green, and blue color components and wherein, said modifying sets the least significant bits within pixel data of the blue components, such modification is also well known in the art the (see column 6, lines 9-41). These claims are therefore rejected on the same rationale as the rejection of claim 1 above.

As per claim 4, Mast substantially discloses rendering pixel data in video RAM on a video display device, (see column 1, lines 40-47).

As per claims 5, 30, and 56, Dwin et al. discloses the limitation of rendering pixel data that is visually similar to the stored pixel data when rendered on a video display device, for example (see column 7, lines 25-61). These claims are therefore rejected on the same rationale as the rejection of claim 1 above.

As per claim 6, Mast discloses the limitation of wherein the pixel data is copied from the video RAM by a screen capture command (column 10, lines 52-66 and columns 11-12).

As per claim 7, Mast discloses the limitation of wherein the pixel data is copied from the video RAM by command to copy screen data to a clipboard (column 10, lines 52-66 and columns 11-12).

As per claims 8, 32, and 60, Mast discloses the limitation of wherein the protected pixel data is pixel data for at least one protected digital image (see fig. 8 and column 10, line 52 through column 12).

As per claim 9, Mast substantially teaches the claimed method of claim 8. **Mast** discloses sending protected image to end user but does not specifically disclose downloading the at least one protected image over the Internet, which is well known in the art.

As per claims 12 and 34, Mast discloses the limitation of wherein the stored pixel data is encrypted pixel data (see column 7, lines 20-47).

As per claims 13 and 35, Mast discloses the limitation of decoding encrypted stored pixel data (see column 9, lines 8-20).

As per claim 10, Mast discloses the limitation of wherein the stored pixel data is encrypted pixel data (see column 7, lines 20-47). **Mast** further discloses that the image files are protected from misappropriation with some form of encryption and suggests to use other encryption schemes than the one disclosed (see column 7, lines 40-47). Therefore, it is apparent to one of ordinary skill in the art, as an encryption scheme, to have the substitute pixel datum encrypted to indicate that they are protected images.

As per claim 11, Mast discloses the limitation of decoding encrypted pixel data (see column 9, lines 8-20).

As per claim 14, Mast teaches the limitations of claim 14 using a method and an apparatus in a computer system (see column 4, lines 19-28). **Claim 14** recites the same limitation as the rejected claim 1 except for incorporating the claimed methods into a system. A computer system has data buses to transfer data for storage, a digital filter to identify and modify

pixel data, and processors to replace or copy information to memory. It is apparent to one skilled in the art that the method disclosed by **Mast** can be applied in a system.

Claims 16, 38, and 68 are similar to the rejected **claim 3** except for incorporating the claimed method into a system. Therefore, **claims 16, 38, and 68** are rejected on the same rationale as the rejection of **claim 3**.

As per claim 17, Mast discloses the claimed system of claim 14. **Claim 17** is similar to the rejected **claim 4**. Therefore, **claim 17** is rejected on the same rationale as the rejection of **claim 4**.

Claims 18, 40, and 70 are similar to the rejected **claim 5** except for incorporating the claimed method into a system. Therefore, **claims 18, 40, and 70** are rejected on the same rationale as the rejection of **claim 5**.

As per claim 19, Mast discloses the claimed system of claim 14. **Claim 19** recites the limitation of wherein said first data bus and said second data bus are distinct data busses. It is apparent to one skilled in the art that a computer system has distinct data buses to transfer data for storage (see column 4, lines 19-28).

As per claim 20, Mast discloses the claimed system of claim 14. **Claim 20** recites the limitation of wherein said first data bus and said second data bus are the same data bus. The fact

of using the same data bus instead of two distinct data buses may reduce cost. However, having one bus may slow down the process of transmitting data, and furthermore, it does not provide any backup if the bus fails. It is apparent to one skilled in the art that a computer system is capable of using either the same bus or distinct data buses (see column 4, lines 19-28).

Claims 21, 41, and 75 are similar to the rejected **claim 8** except for incorporating the claimed method into a system. Therefore, **claims 21, 41, and 75** are rejected on the same rationale as the rejection of **claim 8**.

Claims 22, 42, and 76 are similar to the rejected **claim 9** except for incorporating the claimed method into a system. Therefore, **claims 22, 42, and 76** are rejected on the same rationale as the rejection of **claim 9**.

As per claims 23-26, Mast discloses the claimed system of claim 14. **Claims 23-26** are similar to the rejected **claims 10-13** respectively. Therefore, **claims 23-26** are rejected on the same rationale as the rejection of **claims 10-13**.

As per claim 27, claim 27 recites some of the limitations of the rejected claim 1. Therefore, **claim 27** is rejected on the same rationale as the rejection of **claim 1**.

Claims 31 and 57 are similar to the rejected **claim 5**. Therefore, **claims 31 and 57** are rejected on the same rationale as the rejection of **claim 5**.

Claims 33 and 61 are similar to the rejected **claim 9**. Therefore, **claims 33 and 61** are rejected on the same rationale as the rejection of **claim 9**.

As per claim 36, Mast substantially teaches the limitations of claim 36 using a method and an apparatus in a computer system (see column 4, lines 19-28). **Claim 36** recites the same limitation as the rejected claim 1 except for incorporating the claimed methods into a system. A computer system has data buses to transfer data for storage and a digital filter to identify and modify pixel data. It is apparent to one skilled in the art that the method disclosed by **Mast** can be applied in a system.

Claims 39 and 69 are similar to the rejected **claim 4** except for incorporating the claimed method into a system. Therefore, **claims 39 and 69** are rejected on the same rationale as the rejection of **claim 4**.

Claims 43 and 79 are similar to the rejected **claim 12** except for incorporating the claimed method into a system. Therefore, **claims 43 and 79** are rejected on the same rationale as the rejection of **claim 12**.

Claims 44 and 80 are similar to the rejected **claim 13** except for incorporating the claimed method into a system. Therefore, **claims 44 and 80** are rejected on the same rationale as the rejection of **claim 13**.

As per claim 45, Mast substantially teaches a method for protecting pixel data located in a video RAM from being copied. **Mast** also discloses replacing protected pixel data with substitute pixel data, after instruction to copy pixel data from the video RAM (see column 3, lines 30-49, column 9, lines 59 et seq., and column 10, line 53 through column 11, line 1). (See also column 2, lines 13-25). **Mast** discloses that encryption fails to protect pixel data within the video memory because of the need to be displayed (see column 1, lines 62-66). **Mast** discloses that prior art technique may be applied to provide protection of data until displayed and the present invention will continue to provide security for data transfer request being in the video memory and teaches means of preventing copying of images stored in the picture store of the video display (see abstract and column 3, lines 25-58). **Mast** combines encryption technique with the present invention as an example of prior art protection prior to placing the image in the video memory. **Mast** mentions that other prior art utilizes masking of portions of visual output but fails to design for security purposes (column 2, lines 13-25). **Mast** does not explicitly disclose prior art technique using least significant bits technique for providing protection of pixels data. However, **Dwin et al** in an analogous art discloses a technique for protecting displayed information by modifying the least significant bit to generate control data (see column 8, lines 45-62) and further teaches reading protection data in the lock buffer (non-display section) to determine location in the frame buffer (video memory) where information can be written and ultimately on the display screen (column 3, lines 30-46), which meets the recitation of modifying least significant bits of stored pixel data prior to it's being received by the video RAM, (see also column 7, lines 45-61 and column 8, lines 15-35 and lines 45-63; column 5, lines

22-28). There is suggestion that an alternative to storing the entire frame buffer image (display image) would be to store data representing only the information to be protected in the lock buffer (non-display memory) (column 7, lines 45-48) and discloses "once the lock data is placed in the lock buffer, subsequently writing into the frame buffer (video memory) is controlled by the contents of the lock buffer; protection data is read in the lock buffer and control signal is generated to write data in the frame buffer section, because data to be protected is identified and is already protected, it is obvious that setting of the bits can be applied before writing into the frame buffer. "The specific structure of information shown in the frame buffer is only an example and it is well known within the skill of the art to provide different arrangements of the data" (column 7, lines 25-37). **Dwin et al** further discloses recognizing individual pixel datum as being protected or unprotected based on the least significant bits of the datum without comparison to a template of pixel locations, for example (see column 7, lines 45-61 and column 8, lines 15-35 column 5, lines 22-28) with the advantage that it enables to know which location of the data to be displayed must be protected by setting all the protect bits corresponding to the pixels in the destination for the object (see column 8, lines 14-35 and lines 45-67). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Mast** by modifying least significant bits of stored pixel data prior to its being received by the video RAM and recognizing individual pixel datum as being protected or unprotected based on the least significant bits of the datum as taught by **Dwin et al.** (see column 7, lines 10-40). One skilled in the art would have been motivated to do so because Mast suggests having the image present in the video memory unprotected is susceptible to piracy and one of ordinary skill of the art would have been motivated to utilize the method of **Dwin et al** of

modifying the bits before the image is present in the video memory so it is not susceptible to piracy when it is displayed as suggested by **Mast**. Contrarily to some prior art that provides protection only before displaying data as mentioned in Mast, **Dwin et al** also provides the advantage where data to be displayed and data currently displayed can remain protected by modifying significant pixels to provide control and identification of data locations that need to be protected before displaying on the screen, wherein any portion of the screen may be so protected using a lock protect bit that corresponds to any pixel data that needs to be protected (see column 7, lines 38-61 and column 8, lines 14-35, 45-67), selected areas of the screen can be protected against overwriting (column 7, lines 34-38).

As per claim 46, Mast discloses the limitation of wherein the pixel data is copied from the video RAM by a screen capture command (column 10, lines 52-66 and columns 11-12).

As per claim 47, Mast discloses the limitation of wherein the pixel data is copied from the video RAM by command to copy screen data to a clipboard (column 10, lines 52-66 and columns 11-12).

As per claim 48, Mast discloses the limitation of wherein the stored pixel data is encrypted pixel data (see column 7, lines 20-47). **Mast** further discloses that the image files are protected from misappropriation with some form of encryption and suggests to use other encryption schemes than the one disclosed (see column 7, lines 40-47). Therefore, it is apparent

to one of ordinary skill in the art, as an encryption scheme, to have the substitute pixel datum encrypted to indicate that they are protected images.

As per claim 49, Mast discloses the limitation of decoding encrypted pixel data (see column 9, lines 8-20).

As per claim 50, Mast teaches the limitations of **claim 50** using a method and an apparatus in a computer system (see column 4, lines 19-28). **Claim 50** recites the same limitation as the rejected claim 45 except for incorporating the claimed methods into a system comprising a data bus and a pixel processor. A computer system has data buses to transfer data for storage, and processors to replace individual pixel datum. It is apparent to one skilled in the art that the method disclosed by **Mast** can be applied in a system.

Claim 51 is similar to the rejected **claim 10** except for incorporating the claimed method into a system. Therefore, **claim 51** is rejected on the same rationale as the rejection of **claim 10**.

Claim 52 is similar to the rejected **claim 11** except for incorporating the claimed method into a system. Therefore, **claim 51** is rejected on the same rationale as the rejection of **claim 11**.

As per claim 53, Mast substantially teaches a method for protecting digital images from being copied from a video RAM. **Mast** discloses the steps of modifying the stored pixel data so as to mark it as being protected and thereafter transmitting stored pixel data including the

modified protecting pixel data from a computer memory to a video RAM (see column 7, lines 34-47 see column 3, lines 10-14; column 2, lines 13-25). (See also prior art columns 1-3). **Mast** also discloses the step of identifying protected image within the image in memory that meets the recitation of identifying the protected pixel data within the stored pixel data (see column 3, lines 30-49 and column 10, lines 57-61); and in response to pixel data being copied from the video RAM, replacing individual pixel datum copied from the video RAM, that is protected, with substitute pixel datum (column 3, lines 30-49, column 9, lines 59 et seq., and column 10, line 53 through column 11, line 1); and discloses after instruction to copy pixel data from the video RAM, replacing individual pixel datum that is recognized as being protected, with substitute pixel datum without comparison to a template of pixel locations (column 3, lines 30-49, column 9, lines 59 et seq., and column 10, line 53 through column 11, line 1). **Mast** discloses that encryption fails to protect pixel data within the video memory because of the need to be displayed (see column 1, lines 62-66). **Mast** discloses that prior art technique may be applied to provide protection of data until displayed and the present invention will continue to provide security for data transfer request being in the video memory and teaches means of preventing copying of images stored in the picture store of the video display (see abstract and column 3, lines 25-58). **Mast** combines encryption technique with the present invention as an example of prior art protection prior to placing the image in the video memory. **Mast** mentions that other prior art utilizes masking of portions of visual output but fails to design for security purposes (column 2, lines 13-25). **Mast** does not explicitly disclose prior art technique using least significant bits technique for providing protection of pixels data. However, **Dwin et al** in an analogous art discloses a technique for protecting displayed information by modifying the

least significant bit to generate control data (see column 8, lines 45-62) and further teaches reading protection data in the lock buffer (non-display section) to determine location in the frame buffer (video memory) where information can be written and ultimately on the display screen (column 3, lines 30-46), which meets the recitation of modifying least significant bits of stored pixel data prior to it's being received by the video RAM, (see also column 7, lines 45-61 and column 8, lines 15-35 and lines 45-63; column 5, lines 22-28). There is suggestion that an alternative to storing the entire frame buffer image (display image) would be to store data representing only the information to be protected in the lock buffer (non-display memory) (column 7, lines 45-48) and discloses "once the lock data is placed in the lock buffer, subsequently writing into the frame buffer (video memory) is controlled by the contents of the lock buffer; protection data is read in the lock buffer and control signal is generated to write data in the frame buffer section, because data to be protected is identified and is already protected, it is obvious that setting of the bits can be applied before writing into the frame buffer. "The specific structure of information shown in the frame buffer is only an example and it is well known within the skill of the art to provide different arrangements of the data" (column 7, lines 25-37). **Dwin et al** further discloses recognizing individual pixel datum as being protected or unprotected based on the least significant bits of the datum without comparison to a template of pixel locations, for example (see column 7, lines 45-61 and column 8, lines 15-35 column 5, lines 22-28) with the advantage that it enables to know which location of the data to be displayed must be protected by setting all the protect bits corresponding to the pixels in the destination for the object (see column 8, lines 14-35 and lines 45-67). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Mast**

by modifying least significant bits of stored pixel data prior to its being received by the video RAM and recognizing individual pixel datum as being protected or unprotected based on the least significant bits of the datum as taught by **Dwin et al.** (see column 7, lines 10-40). One skilled in the art would have been motivated to do so because Mast suggests having the image present in the video memory unprotected is susceptible to piracy and one of ordinary skill of the art would have been motivated to utilize the method of **Dwin et al** of modifying the bits before the image is present in the video memory so it is not susceptible to piracy when it is displayed as suggested by **Mast**. Contrarily to some prior art that provides protection only before displaying data as mentioned in Mast, **Dwin et al** also provides the advantage where data to be displayed and data currently displayed can remain protected by modifying significant pixels to provide control and identification of data locations that need to be protected before displaying on the screen, wherein any portion of the screen may be so protected using a lock protect bit that corresponds to any pixel data that needs to be protected (see column 7, lines 38-61 and column 8, lines 14-35, 45-67), selected areas of the screen can be protected against overwriting (column 7, lines 34-38).

Claims 58-59 are similar to the rejected **claims 6-7** respectively. Therefore, **claims 58-59** are rejected on the same rationale as the rejection of **claims 6-7**.

Claims 62-63 are similar to the rejected **claims 10-11** respectively. Therefore, **claims 62-63** are rejected on the same rationale as the rejection of **claims 10-11**.

As per claim 64, Mast discloses the limitation of wherein the protected pixel data is encrypted pixel data (see column 7, lines 20-47).

As per claim 65, Mast discloses the limitation of decoding encrypted stored pixel data (see column 9, lines 8-20).

As per claim 66, Mast teaches the limitations of **claim 66** using a method and an apparatus in a computer system (see column 4, lines 19-28). **Claim 66** recites the same limitation as the rejected claim 53 except for incorporating the claimed methods into a system comprising a data bus and a pixel processor. A computer system has data buses to transfer data for storage, and processors to modify and replace pixel data. It is apparent to one skilled in the art that the method disclosed by **Mast** can be applied in a system.

As per claim 71, Mast discloses the claimed system of claim 66. **Claim 71** recites the limitation of wherein said first data bus and said second data bus are distinct data busses. It is apparent to one skilled in the art that a computer system has distinct data buses to transfer data for storage (see column 4, lines 19-28).

As per claim 72, Mast discloses the claimed system of claim 66. **Claim 72** recites the limitation of wherein said first data bus and said second data bus are the same data bus. The fact of using the same data bus instead of two distinct data buses may reduce cost. However, having one bus may slow down the process of transmitting data and furthermore it does not provide any

backup if the bus fails. It is apparent to one skilled in the art that a computer system is capable of using either the same bus or distinct data buses (see column 4, lines 19-28).

As per claim 73, Mast discloses the claimed system of claim 66. **Claim 73** recites the limitation of wherein said first pixel processor and said second pixel processor are distinct processors. It is apparent to one skilled in the art that a computer system may have distinct processors for different tasks (see also column 4, lines 19-28).

As per claim 74, Mast discloses the claimed system of claim 66. **Claim 74** recites the limitation of wherein said first pixel processor and said second pixel processor are the same processors. The fact of using the same processor instead of two distinct processors may reduce cost. It is apparent to one skilled in the art to have a system using a CPU as a processor to perform all the tasks. It is apparent to one skilled in the art that a computer system is capable of using either the same processor or distinct processors (see also column 4, lines 19-28).

As per claim 77, Mast discloses the claimed system of claim 66 and further discloses the limitation of wherein the stored pixel data is encrypted pixel data (see column 7, lines 20-47). **Mast** further discloses that the image files are protected from misappropriation with some form of encryption and suggests to use other encryption schemes than the one disclosed (see column 7, lines 40-47). Therefore, it is apparent to one of ordinary skill in the art, as an encryption scheme, to have the substitute pixel datum encrypted to indicate that they are protected images.

As per claim 78, Mast discloses the claimed system of claim 66 and further discloses the limitation of decoding encrypted pixel data (see column 9, lines 8-20).

Conclusion

4. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

4.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

cc

Carl Colin
Patent Examiner
May 24, 2006

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100